ON THE EQUATION $\phi(x) + \phi(k) = \phi(x + k)$

Patricia Jones
University of Southwestern Louisiana, Lafayette, LA 70504
(Submitted May 1988)

Solutions of the equation

$$\phi(x) + \phi(k) = \phi(x + k)$$

(where ϕ is Euler's totient function) were considered by Makowski [3]. He showed that at least one solution exists if k is even, or k is not divisible by 3, or

$$k = mF_0^{a_0}F_1^{a_1} \ldots F_s^{a_s},$$

where $F_i = 2^{2^i} + 1$ is the i^{th} Fermat number, $a_i > 1$ for $0 \le i \le s$, F_{s+1} is prime, and $(m, 2F_0F_1 \ldots F_sF_{s+1}) = 1$. He did not determine whether solutions exist for other odd numbers that are divisible by 3. Makowski also raised the question whether there are positive integers for which no solution exists. In particular, he noted that it is not known whether there is a solution for $k = 3$.

This paper provides very severe necessity conditions for x when $k = 3$, and significantly enlarges the set of integers for which at least one solution is known to exist.

Throughout this paper, p, q, and r will denote distinct odd prime numbers.

Lemma 1: If $\phi(n) = 2j$ for $j > 1$ and odd, then $n = p^\alpha$ or $n = 2p^\alpha$.

The proof is given in [1].

Lemma 2: If $\phi(n) = 4j$ for some odd $j > 1$, then n is one of the following: p^α, $2p^\alpha$, $4p^\alpha$, $p^\alpha q^\beta$, or $2p^\alpha q^\beta$.

Proof: Clearly n cannot be divisible by 8 and cannot have more than two distinct odd prime factors.

Theorem I: If $\phi(x) + \phi(3) = \phi(x + 3)$, then

(i) $x = 2p^\alpha$ or $x = 2p^\alpha - 3$, and
(ii) $p > 3$.

Proof: (i) Let $\phi(x) = 2^v j$ and $\phi(x + 3) = 2^m k$ for j, k odd. Then the hypothesis gives us $2^v j + 2 = 2^m k$. Hence, $v = 1$ iff $m \ne 1$.

<u>Case 1</u>. Let $v = 1$. Then $x = p^\alpha$ or $x = 2p^\alpha$ by Lemma 1. $x = p^\alpha$ implies

$$p^\alpha - p^{\alpha-1} + 2 = \phi(p^\alpha + 3),$$

and since $p^\alpha + 3$ is even,

$$\phi(p^\alpha + 3) \le \frac{p^\alpha + 3}{2}.$$

Thus, $p^\alpha + 1 \le 2p^{\alpha-1}$, which is impossible.

<u>Case 2</u>. Let $m = 1$. Then $x = p^\alpha - 3$ or $x = 2p^\alpha - 3$ (Lemma 1). Since $p^\alpha - 3$ is even,

$$\phi(p^\alpha - 3) \le \frac{p^\alpha - 3}{2}.$$

However,

$$\phi(p^\alpha) \ge \frac{2}{3}p^\alpha;$$

so if $x = p^\alpha - 3$, we have

$$\frac{p^\alpha - 3}{2} + 2 \geq \phi(p^\alpha - 3) + \phi(3) \geq \frac{2}{3}p^\alpha,$$

which gives the contradiction $3 \geq p^\alpha$.

(ii) Suppose $p = 3$.

Case 1. Let $x = 2 \cdot 3^\alpha$ for $\alpha > 1$. Then

$$\phi(2 \cdot 3^\alpha) + \phi(3) = \phi(2 \cdot 3^\alpha + 3),$$

so that

$$3^{\alpha-1} + 1 = \phi(2 \cdot 3^{\alpha-1} + 1).$$

Notice that this implies that $2 \cdot 3^{\alpha-1} + 1$ and $\phi(2 \cdot 3^{\alpha-1} + 1)$ are relatively prime; hence, $2 \cdot 3^{\alpha-1} + 1$ is square-free. And since $8 \nmid (3^{\alpha-1} + 1)$, Lemma 2 gives us

$$2 \cdot 3^{\alpha-1} + 1 = q \quad \text{or} \quad 2 \cdot 3^{\alpha-1} + 1 = qr.$$

The supposition $2 \cdot 3^{\alpha-1} + 1 = q$ leads to the contradiction

$$\phi(2 \cdot 3^{\alpha-1} + 1) = 2 \cdot 3^{\alpha-1} = 3^{\alpha-1} + 1.$$

Hence, $2 \cdot 3^{\alpha-1} + 1 = qr$.

Assume $q > r$. Since

$$2\phi(qr) = 2(3^{\alpha-1} + 1) = qr + 1 = 2(qr - q - r + 1),$$

we get $qr = 2q + 2r - 1$. But $r \geq 5$, so $qr > 4q$. Therefore, $2r - 1 > 2q$, which contradicts $q > r$.

Case 2. Let $x = 2 \cdot 3^\alpha - 3$ for $\alpha > 1$. Then

$$2\phi(2 \cdot 3^{\alpha-1} - 1) + 2 = 2 \cdot 3^{\alpha-1} \quad \text{and} \quad \phi(2 \cdot 3^{\alpha-1} - 1) = 3^{\alpha-1} - 1.$$

Hence $2 \cdot 3^{\alpha-1} - 1$ and $\phi(2 \cdot 3^{\alpha-1} - 1)$ are relatively prime, which implies that $2 \cdot 3^{\alpha-1} - 1$ is square-free. Also, since $3 \nmid (3^{\alpha-1} - 1)$, we have $3 \nmid \phi(2 \cdot 3^{\alpha-1} - 1)$. So, if $q \mid (2 \cdot 3^{\alpha-1} - 1)$, then $q \not\equiv 1 \pmod 3$. Thus, $q \equiv 2 \pmod 3$. So,

$$\phi(2 \cdot 3^{\alpha-1} - 1) = (q_1 - 1)(q_2 - 1) \cdots (q_i - 1) \equiv 1 \pmod 3.$$

But $(3^{\alpha-1} - 1) \equiv 2 \pmod 3$. This contradiction completes the proof.

Lemma 3: If $\phi(2p^\alpha) + \phi(3) = \phi(2p^\alpha + 3)$, then $\dfrac{\phi(2p^\alpha + 3)}{2p^\alpha + 3} < \dfrac{1}{2}$.

Proof: $\phi(2p^\alpha + 3) = \phi(2p^\alpha) + \phi(3) = \left(\dfrac{p-1}{p}\right)p^\alpha + 2 < \dfrac{2p^\alpha + 3}{2}$.

Lemma 4: If $\phi(2p^\alpha - 3) + \phi(3) = \phi(2p^\alpha)$, then $\dfrac{\phi(2p^\alpha - 3)}{2p^\alpha - 3} < \dfrac{1}{2}$.

Proof: $\phi(2p^\alpha - 3) = \phi(2p^\alpha) - \phi(3) = \left(\dfrac{p-1}{p}\right)p^\alpha - 2 < \dfrac{2p^\alpha - 3}{2}$.

Lemma 5: Let $S = \{q \mid q \equiv 2 \pmod 3\}$. If n is a positive integer such that every prime factor of n belongs to S and $\phi(n)/n < 1/2$, then n has more than 32 distinct prime factors.

Proof: Calculations show that even if the 32 smallest primes in S all divide n, $\phi(n)/n$ is still greater than 1/2.

Theorem II: If $\phi(x) + \phi(3) = \phi(x + 3)$, then:

(i) x or $x + 3$ has at least 33 distinct prime factors, or
(ii) $x = 2p^\alpha$ for α odd, $p \equiv 2 \pmod 3$, $x > 10^{11}$, and $x + 3$ has at least 9 distinct prime factors.

Proof:

Case 1. Let $x = 2p^{\alpha} - 3$, α even. Suppose $q|x$. Then $2p^{\alpha} - 3 = qv$ for some integer v, and $4p^{\alpha} = 2qv + 6$. And since a is even, 6 is a quadratic residue mod q. Hence, the thirteen smallest primes that can divide x are 5, 19, 23, 29, 43, 47, 53, 67, 71, 73, 97, 101, and 139. Let $x = q_1^{m_1}q_2^{m_2} \ldots q_i^{m_i}$. Calculations show that

$$\frac{1}{2} < \frac{4}{5}\cdot\frac{18}{19}\cdot\frac{22}{23}\cdot\frac{28}{29}\cdot\frac{42}{43}\cdot\frac{46}{47}\cdot\frac{52}{53}\cdot\frac{66}{67}\cdot\frac{70}{71}\cdot\frac{72}{73}\cdot\frac{96}{97}\cdot\frac{100}{101}\cdot\left(\frac{138}{139}\right)^{28}.$$

So if $i \leq 40$, then $\phi(x)/x > 1/2$. But $\phi(x)/x < 1/2$ by Lemma 4. Hence, $i > 40$.

Case 2. Let $x = 2p^{\alpha} - 3$, α odd. Suppose $q|x$ and $q \equiv 1 \pmod 3$. Then we have $\phi(x) \equiv 0 \pmod 3$. So

$$[\phi(x) + \phi(3)] \equiv 2 \pmod 3.$$

But $\phi(x) + \phi(3) = \phi(x + 3)$; hence,

$$\phi(x + 3) = \phi(2p^{\alpha}) = p^{\alpha-1}(p - 1) \equiv 2 \pmod 3.$$

And since α is odd, this is impossible. Thus, if $q|x$, then $q \equiv 2 \pmod 3$. So by Lemmas 4 and 5, x has at least 33 distinct prime factors.

Case 3. Let $x = 2p^{\alpha}$, α even. Suppose $q|(x + 3)$ and $q \equiv 1 \pmod 3$. Then $\phi(x + 3) \equiv 0 \pmod 3$. But

$$\phi(x + 3) = \phi(2p^{\alpha}) + \phi(3) = p^{\alpha-1}(p - 1) + 2.$$

So $p^{\alpha-1}(p - 1) + 2 \equiv 0 \pmod 3$, which implies

$$p^{\alpha-1}(p - 1) \equiv 1 \pmod 3.$$

And since α is even, this is impossible. Hence, if $q|(x + 3)$, then $q \equiv 2$ (mod 3). Thus, by Lemmas 3 and 5, $x + 3$ has at least 33 distinct prime factors.

Case 4. Let $x = 2p^{\alpha}$, α odd, and $p \equiv 1 \pmod 3$. Suppose $q|x + 3$ and $q \equiv 1 \pmod 3$. Then $\phi(x + 3) \equiv 0 \pmod 3$. But

$$\phi(x + 3) = p^{\alpha-1}(p - 1) + 2 \equiv 2 \pmod 3.$$

Hence, every prime divisor of $x + 3$ belongs to $S = \{q|q = 2 \pmod 3\}$. Therefore, by Lemmas 3 and 5, $x + 3$ has at least 33 distinct prime factors.

Case 5. Let $x = 2p^{\alpha}$, α odd, and $p \equiv 2 \pmod 3$. Suppose that $5|(x + 3)$, $q|(x + 3)$, and $q \equiv 1 \pmod 5$. Then $\phi(x + 3) \equiv 0 \pmod 5$, $p^{\alpha} \equiv 1 \pmod 5$, and, since α is odd, $p^{\alpha-1} \equiv \pm 1 \pmod 5$. Therefore,

$$\phi(x + 3) = p^{\alpha} - p^{\alpha-1} + 2 \not\equiv 0 \pmod 5.$$

Hence, the prime factors of $x + 3$ all belong to $S_1 = \{q|q \geq 7\}$ or $5|(x + 3)$ and every other prime divisor of $x + 3$ belongs to $S_2 = \{q|q > 5 \text{ and } q \equiv 1 \pmod 5\}$. Let

$$x + 3 = q_1^{m_1}q_2^{m_2} \ldots q_i^{m_i}.$$

Calculations show that if all q_j belong to S_1 or $q_1 = 5$, and all other q_j belong to S_2, then $\phi(x + 3)/(x + 3) > 1/2$ whenever $i \leq 8$. Therefore, by Lemma 3, $x + 3$ has at least 9 distinct prime factors. Calculations also show that in either case, $x > 10^{11}$.

Makowski did not determine whether solutions exist for $k = 18t \pm 3$ or for $k = 45m$, where $5\nmid m$. The following theorems not only prove that solutions exist for many of these integers, they characterize x for each k.

Theorem III: $\phi(x) + \phi(k) = \phi(x + k)$ has a solution if $k = 3m$ is odd and satisfies any of these conditions:

(i) $p^{\alpha} \| k$, $p^{\beta} = q - 2$, $\alpha > \beta$, and $q \nmid k$;

(ii) $p \| k$, $p = 3q - 4$, and $q \nmid k$;

(iii) $p \| k$, $p = 9q - 16$, and $q \nmid k$;

(iv) $p \| k$, $p = 3^{\alpha}q - 2^{\alpha}r$, $3^{\alpha} - 1 = 2^{\alpha - 1}(r + 1)$, $q \nmid k$ and $r \nmid k$.

Proof:

(i) Let $k = p^{\alpha}j$. Then $\phi(2q^{\alpha-\beta}j) + \phi(p^{\alpha}j) = \phi(qp^{\alpha-\beta}j)$.

(ii) Let $k = 3^{\alpha}pj$. Then $\phi(2^2 \cdot 3^{\alpha}j) + \phi(3^{\alpha}pj) = \phi(q \cdot 3^{\alpha+1}j)$.

(iii) Let $k = 3^{\alpha}pj$. Then $\phi(2^4 \cdot 3^{\alpha}j) + \phi(3^{\alpha}pj) = \phi(q \cdot 3^{\alpha+2}j)$.

(iv) Let $k = 3pj$. Then $\phi(3 \cdot 2^{\alpha}rj) + \phi(3pj) = \phi(3^{\alpha+1}qj)$.

Theorem IV: Let $2^m + 1 = 3^{\alpha}n$ where $(3, n) = 1$ and $\alpha \geq 0$; and suppose there exists a positive integer j such that $j - \phi(j) = n$ and $3^{\alpha}j - 2^{m+1} = p$. Then, if $k = 3pv$ where $(3v, 2pj) = 1$, the equation $\phi(x) + \phi(k) = \phi(x + k)$ has a solution.

Proof: $\phi(2^{m+1} \cdot 3v) + \phi(3pv) = \phi(3^{\alpha+1} \cdot jv)$.

Theorems III and IV provide a solution for 51 of the 91 positive odd integers that are less than 10,000, divisible by 45, and not divisible by 25. They also give solutions for 50 of the 112 k such that $k = 18t \pm 1$ and $k < 1000$. Since the solutions produced by these theorems depend on k being divisible by certain kinds of primes, it seems reasonable to expect that numbers with many prime divisors are much more likely to satisfy the hypotheses of the theorems than the relatively small numbers considered above.

It is not known whether there are solutions for $k = 3p$ where p = 5, 7, 13, 19, 23, 59, 67, 71, 73, 97, 113, 127, 131, 151, 163, 167, 181, or 199. For all other $p < 200$, $k = 3$ has a solution defined in Theorems III and IV.

Theorem IV raises the question: for which n does the equation $n = x - \phi(x)$ have at least one solution? This equation was considered by Erdös [2], but a characterization of all such n has not been found.

The calculations in part (i) of Theorem II could probably be refined to show that x or $x + 3$ must have 40 or more distinct prime divisors. But such a refinement would not be significant, since we have already shown that any solution for $k = 3$ must be very large. Now the real challenge is to prove that $\phi(x) + \phi(3) = \phi(x + 3)$ has no solution.

Finally, we mention two other related, unanswered questions:

1. For which positive integers n does $\phi(x) + \phi(n - x) = \phi(n)$ have at least one solution?
2. For which pairs of positive integers a, b does $\phi(a) + \phi(b) = \phi(a + b)$?

References

1. R. D. Carmichael. "On Euler's ϕ-Function." *Bull. Amer. Math. Soc.* 13 (1907):241-43.
2. P. Erdös. "Über die Zahlen der Form $\sigma(n) - n$ and $n - \phi(n)$." *Elem. Math.* 28 (1973):83-86.
3. A. Makowski. "On Some Equations Involving Functions $\phi(n)$ and $\sigma(n)$." *Amer. Math. Monthly* 67 (1960:668-70.

*****